

REMARKS

Applicants thank the Examiner for the thorough consideration given the present application. Claims 1-16 are pending, of which claims 1, 10-13, 15, and 16 are independent, and claims 1-3, 5, 6, and 10-16 are amended.

The title is amended as requested in the Office Action. The amended title is descriptive and clearly indicative of the invention to which the claims are directed.

The terms identified as informalities in the objection to claim 10 are not misspelled, but rather are acceptable British variations pursuant to MPEP 608.01.

Applicants traverse the rejection of claims 15 and 16 under 35 U.S.C. §101 as being directed to non-statutory subject matter. A programmed computer is a machine under 35 U.S.C. §101. The preamble is part of a claim if it recites structure. See MPEP 2111.02, "Preamble Statements Limiting Structure," and the decisions cited therein, i.e., *Corning Glass Works v. Sumitomo Elec. U.S.A., Inc.*, 868 F.2d 1251, 1257, 9 USPQ2d 1962, 1966 (Fed. Cir. 1989); *Pac-Tec Inc. v. Amerace Corp.*, 903 F.2d 796, 801, 14 USPQ2d 1871, 1876 (Fed. Cir. 1990); and *In re Stencel*, 828 F.2d 751, 4 USPQ2d 1071 (Fed. Cir. 1987), and 1073, 828 F.2d at 754).

Consequently, the requirement in the preamble of claims 15 and 16 for "A computer" is a **structural** limitation that cannot be

ignored. There is a connection between the computer of the preamble and the programmed steps that follow. If the rejection is maintained, the Examiner is requested to cite an authority in support of the position that a programmed computer for performing certain steps does not comply with the requirements of 35 U.S.C. §101.

Claims 13 and 14 are amended to define a processor for generating a digital credential index to ensure compliance with 35 U.S.C. §101.

Claims 1-3, 5, 6, and 10-16 are amended for clarity. In particular, the independent claims are amended to indicate that the index includes the index elements set forth in the specification, especially user-provided information (a) about the credential and (b) differing substantially from the credential such that the credential is not disclosed by the index. Although Applicants believe specifying what the index includes is not necessary because the specification indicates the index includes these elements, such a statement is included for clarity. Other clarifying amendments that recite to what the operations are responsive are also included.

Applicants traverse the rejection of claims 1-16 under 35 U.S.C. §102(b) as being anticipated by Spies et al. (U.S. 5,689,565). The pending claims patentably distinguish over Spies at least by requiring an index to include user-provided information (a) about the

credential and (b) differing substantially from the credential such that the credential is not disclosed by the index.

Consideration of the operation of the Spies device indicates Spies does not anticipate. During the registration process (FIG. 1), Spies' computing units 24(a)-24(c) at participants 22(a)-22(c) are each programmed to generate and send a registration packet over the communication system (as represented by communication paths 30(a)-30(c)) to credential binding server 28 at trusted credential authority 26. Credential binding server 28 (not the user or participant) is programmed to produce unique credentials for each participant based upon registration packet and to send credentials 32(a)-32(c) back over the communication system (as represented by communication paths 34(a)-34(c)) to multiple computing units 24(a)-24(c). These credentials are digitally signed by the trusted credential authority and are used to identify and authenticate other participants during the commerce transaction. See column 6, lines 44-57.

Each registration packet contains general information about the participant. For example, the registration packet includes identification information (e.g., name and location), public cryptography keys unique to the participant and a digital signature of the participant. See column 8, lines 18-28.

FIG. 4 is a flow diagram of steps for generating the registration packet. At steps 70 and 72, the computing unit 24 generates two asymmetric pairs of public and private cryptography keys. An "asymmetric" key algorithm involves two separate keys, e.g., one key to encrypt and one to decrypt. In a public key system, the public key is distributed to other parties, and the private key is maintained in confidence. The asymmetric public and private keys provide two results: First, only the holder of the private key can decrypt a message that is encrypted with the corresponding public key. Second, if another party decrypts a message using the public key, that party can be assured that the message was encrypted by the private key and thus originated with someone (presumably the holder) of the private key. See column 8, lines 49-57.

At step 74, the participant generates a digital signature that is unique to the participant and to the message. The digital signature is computed by hashing the data contained in the registration packet. A hash function is a mathematical function that converts an input data stream into a fixed-size, often smaller, output data stream that is representative of the input data stream. Once the hash is computed, it is encrypted by the computing unit with the private encryption key of the signaling pair (step 76 of FIG. 4). See column 9, lines 3-11.

At step 78, both public keys of the signing pair and the key exchange pair are encrypted with a symmetric cipher using a randomly selected bulk data symmetric encryption key. In a "symmetric" cipher, the encryption key can be calculated from the decryption key, and vice versa. In many cases, the encryption key and the decryption key are the same. See column 9, lines 30-37. In step 78, the data to be included in the registration packet is encrypted with the same or additional symmetric keys. See column 9, lines 50-58.

From the foregoing, it can readily be seen that Spies does not disclose (1) a sender generating or sending index that refers to a credential (per claims 1 and 10) or (2) a computer-readable memory or computer that (a) responds to a user by a communication to a recipient of a credential index having an index that refers to a credential (per claims 11 ad 15) or (b) receives from a sender a credential index having an index that refers to a credential (per claims 12 and 16), or (3) a processor that provides such an index (per claim 13), wherein the index includes the previously discussed user-provided information (a) about the credential and (b) that differs substantially from the credential.

In addition, Spies does not disclose a recipient or service authorizer selecting a credential from such an index (per claims 1 and 10). In Spies, once the symmetric key is recovered, the credential binding server 28 uses it to decrypt the participants'

public keys and other data contained in the registration packet (step 92 in FIG. 5). Next, at step 94, credential binding server 28 decrypts the hash of the participant using the recovered participant's public signing key. This yields the hash, dS, as computed and concealed (encrypted) by the originating participant.

Credential binding server 28 then performs a two-step verification technique to verify that the packet actually originated from the participant. At step 96, credential binding server 28 recalculates the participant's digital signature by hashing the data contained in the decrypted registration packet by using the same hashing function as that employed by the participant. The recalculated hash is then compared with the decrypted hash received as a digital signature, i.e., privately encrypted hash, in the registration packet (step 98 in FIG. 5). If the two hashes match, the credential binding server is advised that the registration packet was signed by the participant and that the contents have not been subsequently altered.

After credential binding server 28 verifies the registration packet as belonging to the participant, the next step 56 (FIG. 3) in the registration process is to generate a credential for the participant, **not** the sender as now required by Applicants' claims. Each credential is unique to a particular participant and is used in future transactions to identify the participants and for

authenticating the participants to each other. See column 10, lines 64 and 65. The credential generated by the credential binding server contains the participant's public signing key, public key exchange key, unique identifiers, validity dates, owner information, issuer information, and information about the participant determined in advance by owners and controllers of the particular commerce environment.

At step 58, the credential binding server 28 attaches a digital signature of the trusted credential authority 26 to the credential. The digital signature is generated by encrypting a hash of the credential using the private key of the trusted credential authority 26. The binder's digital signature is used by the participants during transactions to verify that communications are between authorized participants, who are registered with the trusted credential authority. At step 60, the signed credential is transferred from the credential binding server 28 back over the communications system to the individual computing units 24(a), 24(b), and 24(c) at respective participants 22(a), 22(b), and 22(c). The transfer is illustrated in FIG. 1 by the signed credentials 32(a)-32(c) being returned to the computing units along communication paths 34(a)-34(c).

Spies verifies the authenticity by credential binding server 28 using the steps of FIG. 5 and some steps of FIG. 3. See column 10, line 18, through column 11, line 20.

Based on the foregoing, Spies does not include the requirement of a (1) recipient (claim 1) or (2) service authority (claim 10) or (3) computer memory (claim 12) or (4) computer programmed to (1) select a credential from an index of a credential provided by a user and (2) communicate to the user an indication of the selected credential.

Further, Spies does not disclose the sender responding to the indication by the recipient (amended claim 1) or the service authorizer (amended claim 10) of the selected credential communicated by the recipient or service authorizer by providing to the recipient or authorizer a credential corresponding to the selected credential.

Accordingly, independent claims 1, 10-13, 15, and 16 are allowable. Claims 2-9 and 14 are also allowable due to their dependence on allowable independent claims, as well as for the additional limitations provided by these claims. Therefore, all claims are allowable.

In view of the foregoing amendments and remarks, favorable reconsideration and allowance are respectfully requested and deemed in order.

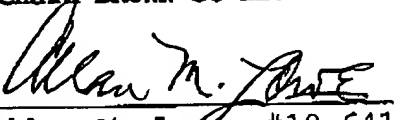


To the extent necessary, Applicants hereby request any required extension of time not otherwise requested and hereby authorize the Commissioner to charge any prescribed fees not otherwise provided for, including application processing, extension, and extra claims fees, to Deposit Account No. 08-2025.

Respectfully submitted,

Richard BROWN et al.

By:

  
Allan M. Love, #19,641

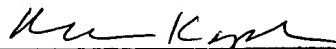
**HP IPA**

P. O. Box 272400  
Fort Collins, CO 80527-2400  
703-684-1111 telephone  
970-898-0640 telecopier  
AML:rk

**Certificate of Mailing**

I hereby certify this correspondence is  
being deposited with the United States Postal Service as  
first class mail in an envelope addressed to: (Commissioner for  
Patents P.O. Box 1450 Alexandria, VA 22313-1450)

On ~~February~~ April 13, 2005



Roseanna Kaplan